AMENDMENTS TO THE CLAIMS

~~[c1]~~1. (Currently amended) In a computer system providing access to at least one secure resourcc upon authentication of a user where said user authentication is performed by an authentication server in remote communication with a client in use by said user, a method of saving said user authentication for use when said authentication server is unavailable, the method comprising the steps of:

–submitting a user authentication request to said authentication server;

–in response to a successful user authentication;

–receiving an authenticated user credential which Is unique to said user;

–storing said authenticated credential on said client utilizing a security method to prevent tampering with the credential;

–using said authenticated credential to access said at least one secure resource;

in response to an unsuccessful user authentication:

determining whether said authentication server is in operative communication with said client;

in response to a determination that said authentication server is not in operative communication with said client:

searching said client for a stored authenticated credential corresponding to said user;

in response to finding an authenticated credential corresponding to said user, using said stored authenticated credential to access said at least one secure resource while said authentication server is not in operative communication with said client; and

in response to not finding an authenticated credential corresponding to said user, failing the user authentication request.

~~[c2]~~2. (Currently amended) The method of claim 1 further comprising the steps of:

~~—in response to an unsuccessful user authentication:~~

~~—determining whether said authentication server is in operative communication with said client;~~

~~— in response to a determination that said authentication server is not in operative communication with said client:~~

~~———searching said client for a stored authenticated credential corresponding to said user;~~

~~——— in response to finding an authenticated credential corresponding to said user, using said stored authenticated credential to access said at least one secure resource;~~

~~in response to not finding an authenticated credential corresponding to said user, failing the user authentication request;~~

–in response to a determination that said authentication server is in operative communication with said client:

–erasing from said client any stored authenticated credential corresponding to said user; and

–failing said user authentication request.

~~[c3]~~3. (Currently amended) The method of claim 2 further comprising the step of:

—implementing a set of security policies limiting the use of authenticated credentials stored on said client to access said at least one secure resource depending on a defined sensitivity of said at least one resource.

~~[c4]~~4. (Currently amended) The method of claim 1 wherein said security method is encryption of the credential.

~~[c5]~~5. (Currently amended) The method of claim 1 wherein said security method is Public Key Infrastructure.

~~[c6]~~6. (Currently amended) The method of claim 1 wherein said security method is hardware based Public Key Infrastructure.

~~[c7]~~7. (Currently amended) The method of claim 2 wherein said security method is encryption of the credential.

~~[c8]~~8. (Currently amended) The method of claim 2 wherein said security method is Public Key infrastructure.

~~[c9]~~9. (Currently amended) The method of claim 2 wherein said security method is hardware based Public Key Infrastructure.

~~[c10]~~10.(Currently amended) In a computer system providing access to at least one secure resource upon authentication of a user where said user authentication is performed by an authentication server in remote communication via a secure gateway with a client in use by said user, a method of caching said user authentication for use when said authentication server is unavailable, the method comprising the steps of:

–submitting a user authentication request to said authentication server;

–in response to a successful user authentication;

–receiving an authenticated user credential which is unique to said user;

–storing said authenticated credential on said client utilizing a security method to prevent tampering with the credential;

–storing said authenticated credential on said gateway utilizing a security method to prevent tampering with the credential;

–using said authenticated credential to access said at least one secure resource~~.~~;

in response to an unsuccessful user authentication:

determining whether said authentication server is in operative communication with said client;

in response to a determination that said authentication server is not in operative communication with said client;

determining whether said gateway is in operative communication with said client;

in response to a determination that said gateway is not in operative communication with said client:

searching the client for an authenticated credential corresponding to said user;

in response to finding an authenticated credential corresponding to said user, using said authenticated credential to access said at least one secure resource while said gateway is not in operative communication with said client;

in response to not finding an authenticated credential corresponding to said user, failing the user authentication request.

~~[c11]~~11. (Currently amended) The method of claim 10 further comprising the steps of:

~~in response to an unsuccessful user authentication:~~

~~determining whether said authentication server is in operative communication with said client;~~

~~in response to a determination that said authentication server is not in operative communication with said client;~~

~~determining whether said gateway is in operative communication with said client;~~

~~in response to a determination that said gateway is not in operative communication with said client:~~

~~searching the client for an authenticated credential corresponding to said user;~~

~~in response to finding an authenticated credential corresponding to said user, using said authenticated credential to access said at least one secure resource;~~

~~in response to not finding an authenticated credential corresponding to said user, failing the user authentication request;~~

–in response to a determination that said gateway is in operative communication with said client:

–searching the gateway for an authenticated credential corresponding to said user;

–in response to finding an authenticated credential corresponding to said user, using said authenticated credential to access said at least one secure resource;

–in response to not finding an authenticated credential corresponding to said user, failing the user authentication request;

–in response to a determination that said authentication server is in operative communication with said client:

–erasing from the client any authenticated credential corresponding to said user;

–erasing from the gateway any authenticated credential corresponding to said user; and

–failing the user authentication request.

~~[c12]~~12. (Currently amended) The method of claim 11 further comprising the step of:

–implementing a set of security policies limiting the use of authenticated credentials stored on said client or on said gateway to access said at least one secure resource depending on a defined sensitivity of said at least one resource.

~~[c13]~~13. (Currently amended) The method of claim 10 wherein said security method is encryption of the credential.

~~[c14]~~14. (Currently amended) The method of claim 10 wherein said security method is Public Key Infrastructure.

~~[c15]~~15. (Currently amended) The method of claim 10 wherein said security method is hardware based Public Key Infrastructure.

~~[c16]~~16. (Currently amended) The method of claim 11 wherein said security method is encryption of the credential.

~~[c17]~~17. (Currently amended) The method of claim 11 wherein said security method is Public Key Infrastructure.

~~[c18]~~18. (Currently amended) The method of claim 11 wherein said security method is hardware based Public Key Infrastructure.